REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1-6, 12-15, 21 and 22 are presently active. Claims 7-11 are withdrawn, and Claims 23-79 were previously canceled without prejudice. Claims 1, 5, 12, 21, and 22 have been presently amended. No new matter was added.

In the outstanding final Office Action, Claims 1-6, 12-15, and 21-22 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,289,450 to Pensak et al.

Statement of Summary of the Interview: Applicants acknowledge with appreciation the courtesy of Examiner Milia to discuss this application with Applicants' representative on October 16, 2008 as substantially summarized hereinafter. During the interview, the discussions were focused on the subject matter of dependent Claim 4 which specifies that the print requirement is obtained from the decrypted document file. Examiner Milia interpreted Pensak et al's option of including a watermark to indicate that in Pensak et al the segments later decrypted at a viewing user contained the watermark. In the examiner's view, this was a disclosure of a printing requirement including at least one security requirement. While this position does not seem completely supported (as would be needed for a proper anticipation rejection), no agreement on patentability on this point was reached during the interview.

Claim Summary: Claim 1 as amended recites:

> 1. A document printing program encoded on a computer readable medium, comprising the codes of:
> obtaining ***a password*** and a print requirement associated with a document file; and
> compulsory executing of the print requirement when the document file is printed out,

> wherein the print requirement sets a print mode including at least one security requirement to be executed to a to-be-printed document, ***and the password is utilized to generate a key for encryption and decryption of the document file***. [Emphasis added.]

Applicants' specification describes on pages 15 and 16 the use of a password for encryption and decryption of the secured document.

The art deficiencies: Without comment as to the correctness of the Office Action's comparison of all the previously filed claims to Pensak et al but rather in an effort to expedite the present application to allowance, Applicants respectfully invite the examiner's attention the following description in Pensak et al.

Pensak et al describe at col. 8, lines 19-45, that:

> The Application Interface 230 will check to see if the user is logged onto the remote server 206. If the viewing user 216 has not logged onto the remote server, the Application Interface 230 provides a pop-up window so that the user can log in to the server. An SSL tunnel and session key are negotiated, 1056, 1058. The viewing user's computer 224 provides login and authentication information to the server 206, 1060. Once logged into the server 206, the Application Interface 230 requests access to the document or information 1062 by asking the server 206 for the decryption key for the first segment of the document or information to be accessed. The server 206 uses the segment ID to check the database to find the policies associated with the segment and thus to determine whether the viewing user 216 is authorized to access this segment or the document as a whole.
>
> If the viewing user 216 is not authorized to access the segment, the viewing user 216 is so informed. If the user 216 is authorized to access the segment, the server 206 sends the decryption key and options for that segment to the Application Interface 230 at the viewing user's computer 224 and the Application Interface 230 decrypts the segment using the decryption key. After decrypting the segment, the Application Interface 230 immediately discards/destroys the key, renders the decrypted segment to the screen, and then destroys the decrypted version of the segment. When the viewing user moves to a different segment, the process is repeated.

Thus, in Pensak et al, the status of the viewing user is checked. If he is an authorized viewer, the segments along with decryption keys are provided so that the authorizing user can

view segment by segment. While Pensak et al describe at col. 2, lines 63-67, the defining of a local user profile by including "password and other identifying information" and while Pensak et al describe at col. 8, line-67, to col. 9, line 1, that "all records maintained in the central database 234 are encrypted and the database is password protected," there is no disclosure or suggestion in Pensak et al for a password being used to generate a key for encryption and decryption of the document file. Rather, the password in Pensak et al is merely used for security protection.

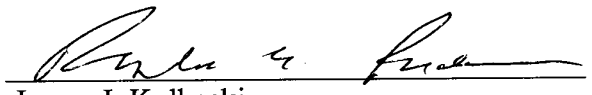
M.P.E.P. § 2131 requires for anticipation that each and every feature of the claimed invention must be shown in as complete detail as is contained in the claim. M.P.E.P. § 2123 I states that a reference may be relied on for all it would have reasonably suggested to one having ordinary skill in the art, including non-preferred embodiments.

Thus, with the above-noted feature not having been disclosed or reasonably suggested in Pensak et al, independent Claims 1, 12, 21, and 22 (and the claims dependent therefrom) patentably define over Pensak et al.

Conclusion: In light of the above discussions, the outstanding grounds for rejection are believed to have been overcome. The application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbaski
Attorney of Record
Registration No. 34,648

Ronald A. Rudder, Ph.D.
Registration No. 45,618

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)